Universidade de Brasília Faculdade UnB Gama

Criptografia e Segurança de Redes
Trabalho 4

Alunos:	Matrículas:
João Paulo Nunes Soares	15/0038267
Josué Nascimento da Silva	15/0038933

- INSTRUÇÕES DE USO
  - ✔ **Exercício 1**
    - ✔ Para compilar o arquivo execute na pasta do arquivo: **gcc ex1.c -lm -o rsa** .
    - ✔ Para executar o programa execute: **./rsa**
    - ✔ Após executar entre com os valores de q , p , e , caso os valores sejam aceitos para gerar um chave o programa irá pedir para digitar o path de onde se encontra o arquivo, caso contrario irá indicar que a chave gerada é invalida parando assim a execução.
  - ✔ **Exercício 2**
    - ✔ Para executar o arquivo digite **python3 ex2.py** .
    - ✔ Insira os valores solicitados.
  - ✔ **Exercício 3**
    - ✔ Certifique-se que o arquivo ex2.py encontra-se no mesmo diretório.
    - ✔ Para executar o arquivo digite **python3 ex3.py**
    - ✔ Insira os valores solicitados no formato correto.
  - ✔ **Exercício 4**
    - ✔ Não foi implementado corretamente, por isso não foi entregue

- LIMITAÇÕES CONHECIDAS
  - ✔ **Exercício 1**
    - ✔ Os valores de p q devem ser primos e de forma que o produto deles de abaixo de 255, pois era limitação do exercicio criptografar caracteres da tabela ascii
    - ✔ Caso o local onde encotra-se o arquivo seja digitado errado o programa apresentará instabilidades e ele deve conter no maximo 30 caracteres.

- **Exercício 2**
  - O exercício 2 não apresenta limitações conhecidas, porém vale ressaltar que sua execução pode demorar dependendos dos valores inseridos.

- **Exercício 3**
  - Os valores devem ser inseridos no formato solicitado, como por exemplo , um ponto deve ser inserido no formato (1,1).
  - Considera-se que os valores correspondentes aos pontos G e P inseridos são válidos, onde as validações referentes a presença dos mesmos na curva descrita pela equação e pelos outros valores não são realizadas.
  - Caso o arquivo ex2.py não esteja presente no mesmo diretório, o programa apresentará erros em seu funcionamento.

CASOS DE TESTE

- Exercício 1
- Exercício 2

```
Insira o valor A: 1
Insira o valor B: 1
Insira o valor P: 23
Ponto: (0, 1)   Ordem:  28
Ponto: (0, 22)   Ordem:  28
Ponto: (1, 7)   Ordem:  28
Ponto: (1, 16)   Ordem:  28
Ponto: (3, 10)   Ordem:  28
Ponto: (3, 13)   Ordem:  28
Ponto: (4, 0)   Ordem:  2
Ponto: (5, 4)   Ordem:  7
Ponto: (5, 19)   Ordem:  7
Ponto: (6, 4)   Ordem:  14
Ponto: (6, 19)   Ordem:  14
Ponto: (7, 11)   Ordem:  14
Ponto: (7, 12)   Ordem:  14
Ponto: (9, 7)   Ordem:  28
Ponto: (9, 16)   Ordem:  28
Ponto: (11, 3)   Ordem:  4
Ponto: (11, 20)   Ordem:  4
Ponto: (12, 4)   Ordem:  14
Ponto: (12, 19)   Ordem:  14
Ponto: (13, 7)   Ordem:  7
Ponto: (13, 16)   Ordem:  7
Ponto: (17, 3)   Ordem:  7
Ponto: (17, 20)   Ordem:  7
Ponto: (18, 3)   Ordem:  28
Ponto: (18, 20)   Ordem:  28
Ponto: (19, 5)   Ordem:  28
Ponto: (19, 18)   Ordem:  28
Ponto de maior ordem (Ordem,(Xp,Yp)):  (28, (19, 18))
Quantidade de pontos: 27
```

Caso de Teste presente no livro texto da Disciplina

✔ Exercício 3

```
Insira o valor A: 0
Insira o valor B: -4
Insira o valor P: 4177
PONTO BASE G:
        Insira o ponto no formato (x,y): (8,838)
PONTO A SER CIFRADO P:
        Insira o ponto no formato (x,y): (2763,806)
======= MENU =======
1- Criptografa
2- Descriptografa
3- Finalizar
Opcao: 1
Insira a chave publica do destinatario para cifracao
        Insira o ponto no formato (x,y): (1050,2151)
Insira um valor inteiro aleatorio: 41
Pontos C1 e C2:  ((2626, 1237), (2715, 488))
======= MENU =======
1- Criptografa
2- Descriptografa
3- Finalizar
Opcao: 2
Insira o ponto C1 no formato (x,y): (2626, 1237)
Insira o ponto C2 no formato (x,y): (2715, 488)
Insira a chave privada para decifrar: 101
Ponto decifrado P':  (2763, 806)
======= MENU =======
1- Criptografa
2- Descriptografa
3- Finalizar
Opcao: 3
```

Caso de teste presente no slide da **Aula 10b – Criptografia de Curva Elíptica**